UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,213	12/07/2005	Max De Groot	032326-296	8823

21839 7590 01/26/2009

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
TORRES, MARCOS L	

ART UNIT	PAPER NUMBER
2617	

NOTIFICATION DATE	DELIVERY MODE
01/26/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/529,213	DE GROOT, MAX	
	Examiner	Art Unit	
	MARCOS L. TORRES	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 10-20-08 have been fully considered but they are not persuasive.

2. Applicant asserts that the office action is incorrect in its assessment that two keys are being used, because the same key must be generated at both the sending and the receiving terminals; although the applicant did indicate which sections of the reference are being used to affirm their position; the examiner stated as correctly pointed by the applicant, that they were two keys one in the sending terminal and another for receiving, which may or not be the same [note that if it would Aura would have explicitly stated they were different keys it would have been a 102 rejection]. However, applicant asserts that the references are not combinable, the examiner disagrees. As stated in the prior office action choosing between asymmetrical or symmetrical algorithm is a design choice within the knowledge of one of the ordinary skills in the art, commonly used to enhance security by the use of public and private keys and using well-known existing algorithm such as RSA, ECDSA as suggested by Labaton in par. 0011.

3. The rest of the argument they fall for the same reasons as shown in paragraph 2 above. The current rejection in record stands.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura 6373949 in view of Labaton US 20060005028A1.

As to claim 1, Aura discloses a process to identify a user of the terminal resource by a server resource in a telecommunication network, using a first identifier, where an encryption algorithm with a key is implemented in the terminal resource (see col. 3, line 54 – col. 4, line 5), comprising the following steps: generating a random number in the user terminal resource (see fig. 5, step 501); determining in the terminal resource of a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the encryption algorithm to which at least the random number is applied (see fig. 5, items 502-503) transmitting the second identifier to the server resource, and in the server resource, retrieval of retrieving the first

identifier at least by executing the encryption algorithm to which a key and, at least partially, the second transmitted identifier are applied, so that the server resource verifies that the first retrieved identifier is written into a memory of the server resource (see fig. 5, items 505-506; col. 4, line 36 – col. 5, line 50). Aura does not specifically disclose using an asymmetrical algorithm. However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 2, Aura discloses a process in which the at least one authentication further including the step of authenticating the terminal resource by the server resource (see fig. 5, items 505-506).

As to claim 3, Aura discloses a process to identify a user of the terminal resource by a server resource in a telecommunication network, using a first identifier, where an encryption algorithm with a key is implemented in the terminal resource (see col. 3, line 54 – col. 4, line 5), comprising the following steps: generating a random number in the user terminal resource (see fig. 5, step 501); determining in the terminal resource of a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the encryption algorithm to which at least the random number is applied (see fig. 5, items 502-503) a process in which the determination in the terminal resource includes application of the generated random

number to the encryption algorithm with the public key to produce an encrypted random number, application of the generated random number and of the first identifier to encryption algorithm implemented in the terminal resource, to produce an encrypted identifier, and concatenation of the encrypted random number and of the encrypted identifier in the second identifier; transmitting the second identifier to the server resource, and in the server resource, retrieval of retrieving the first identifier, and wherein the retrieval in the server resource includes application of the encrypted random number to the encryption algorithm with the key, in order to retrieve the generated random number, and application of the retrieved random number, and of the encrypted identifier to the encryption algorithm, in order to retrieve the first identifier , so that the server resource verifies that the first retrieved identifier is written into a memory of the server resource (see fig. 5, items 501-506; col. 4, line 36 – col. 5, line 50). Aura does not specifically disclose using an asymmetrical algorithm. However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 4, Aura discloses a process to identify a user of the terminal resource by a server resource in a telecommunication network, using a first identifier, where an encryption algorithm with a key is implemented in the terminal resource (see col. 3, line

54 – col. 4, line 5), comprising the following steps: generating a random number in the user terminal resource (see fig. 5, step 501); determining in the terminal resource of a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the encryption algorithm to which at least the random number is applied (see fig. 5, items 502-503); wherein the determination in the terminal resource includes application of the generated random number concatenated to the first identifier, to the asymmetrical algorithm with the public key to produce the second identifier, transmitting the second identifier to the server resource, and in the server resource, retrieval of retrieving the first identifier wherein the retrieval in the server resource includes application of the second identifier to the cyber algorithm with the key in order to retrieve the first identifier, so that the server resource verifies that the first retrieved identifier is written into a memory of the server resource (see fig. 5, items 501-506; col. 4, line 36 – col. 5, line 50)..Aura does not specifically disclose using an asymmetrical algorithm. However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 5, Aura discloses everything as explained above except for the process further including the steps of changing the public key and the private key for the asymmetrical algorithm in the server resource, and downloading of the changed public

key from the server resource to the terminal resource. Labaton discloses process further including the steps of changing the public key and the private key for the asymmetrical algorithm in the server resource, and downloading of the changed public key from the server resource to the terminal resource (see par. 0049), thereby increasing the security.

As to claim 6, Aura discloses a process wherein the generation of the random number is periodic (recurring, repeated) in the terminal resource (see col. 5, lines 46-50).

As to claim 7, Aura discloses a process wherein the generation of the random number occurs following activation of a service application (transfer of subscriber identity, col. 4, lines 25-51).

As to claim 8, Aura discloses a user terminal resource identifying itself, or identifying a user of the latter, to a server resource, through a telecommunication network using a first identifier, an encryption algorithm with a key implemented in the terminal resource, comprising: a resource to generate a random number (see fig. 5, item 501), and a resource, to determine a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the encryption algorithm to which at least the random number is applied in order to transmit the second identifier to the server resource (see fig. 5, items 502-503), which retrieves the first identifier at least by executing the encryption algorithm to which a key and, at least partially, the second identifier are applied, and which verifies that the first retrieved identifier is written into a memory of the server resource (see fig. 5, items 505-

506; col. 4, line 36 – col. 5, line 50). Aura does not specifically disclose using an asymmetrical algorithm. However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 9, Aura discloses a user terminal resource which wherein the resource to generate a random number and the resource to determine a second identifier are included in a portable electronic object of the chip card type (see col. 4, lines 48-51).

As to claim 10, Aura discloses method for identifying at least one of a terminal and a user of the terminal to a server in a telecommunications network, comprising the following steps: generating a random number in the terminal (see fig. 5, item 501); applying said random number and a first identifier associated with said terminal to at least one cyber algorithm in said terminal, using a key, to generate a second identifier that is based upon a combination of said random number and said first identifier (see fig. 5, item 502-503); transmitting said second identifier to said server; applying said second identifier to said cyber algorithm in said server, using a key, to derive said first identifier; and authenticating said terminal or said user in the server, using the derived first identifier (see fig. 5, items 505-506; col. 4, line 36 – col. 5, line 50). Aura does not specifically disclose using an asymmetrical algorithm. However, note that two keys are

being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claims 11-12, Aura discloses the method wherein said random number is applied to said cyber algorithm in said terminal, together with said key, to generate a first result (see fig. 5, item 502), and said first identifier is applied to a second, symmetric (related) algorithm in said terminal, together with a key, to generate a second result, and wherein said second identifier comprises a combination of said first and second results (see fig. 5, item 503). Aura does not specifically disclose using an asymmetrical algorithm (using public private keys). However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 13, Aura discloses the method wherein said second identifier comprises a concatenation of said first and second results (see fig. 5, items 502-503).

As to claim 14, Aura discloses the method wherein said random number is combined with said first identifier, and the combination of said random number and said first identifier is applied as an input to said cyber algorithm in said terminal, together with said key, to generate said second identifier (see fig. 5, items 502-503). Aura does not specifically disclose using an asymmetrical algorithm (using public private keys). However, note that two keys are being used one for encrypting and the other for decrypting. In an analogous art, Labaton discloses using an asymmetrical algorithm (see par.0036, 0068), thereby using a public and private keys. Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to use an asymmetrical algorithm for the simple purpose of using existing algorithm such as RSA, ECDSA and increase the security of the data.

As to claim 15, Aura discloses the method wherein said combination comprises a concatenation of said random number and said first identifier (see fig. 5, items 502-503).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARCOS L. TORRES whose telephone number is (571)272-7926. The examiner can normally be reached on 9:30 am - 6:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, George Eng can be reached on 571-252-7495. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/George Eng/
Supervisory Patent Examiner, Art Unit 2617

/Marcos L Torres/
Examiner, Art Unit 2617